

- 18 -

Claims

1. A system for use of internet authentication technology to provide UMTS authentication, the system
5 comprising:

Serving GPRS Support Node (SGSN) means in a UMTS network; and

RADIUS server means,
the SGSN means and the RADIUS Server means being adapted
10 to support signalling therebetween whereby authentication of a User Subscriber Identity Module (USIM) may be performed in the RADIUS Server means.

2. The system of claim 1 wherein the SGSN means is
15 integrated with Radio Network Controller (RNC) means in Integrated Network Controller (INC) means.

3. The system of claim 1 or 2 wherein the UMTS network comprises a UMTS Terrstril Radio Access Network (UTRAN).
20

4. The system of any preceding claim wherein the SGSN means is adapted to send an Access-Request RADIUS message to request a UMTS Authentication Vector from the RADIUS server means.
25

5. The system of any preceding claim wherein the RADIUS Server means is adapted to generate authentication and keying material so as to authenticate a USIM within a UMTS UE, according to UMTS standards.
30

- 19 -

6. The system of claim 5 wherein the RADIUS Server means is adapted to implement the MILENAGE algorithm.

7. The system of claim 5 or 6 wherein the RADIUS Server means is adapted to generate, using anti-replay-attack dynamic data, a UMTS Authentication Vector, for use by the SGSN means.

8. The system of claim 5 when dependent on claim 4 wherein the RADIUS Server means is adapted to support dynamic sequence number (SQN).

9. The system of any preceding claim wherein the RADIUS Server means is adapted to generate a UMTS Authentication Vector in a RADIUS attribute within an Access-Accept RADIUS message for sending to the SGSN means.

10. The system of any preceding claim wherein the SGSN means is adapted to receive a UMTS Authentication Vector in a RADIUS Access-Accept message.

11. The system of any preceding claim wherein the SGSN means is adapted to send information to re-synchronise anti-replay-attack information within the USIM with the RADIUS Server means.

12. The system of claim 11 when dependent on claim 4 wherein SGSN means is adapted to send a UMTS-Resynchronisation-Token attribute in the Access-Request RADIUS message.

- 20 -

13. The system of claim 12 wherein the RADIUS Server means is adapted to reset anti-replay-attack dynamic data in-line with the USIM in response to the data received in the UMTS-Resynchronisation-Token.

5

14. The system of claim 13 wherein the RADIUS Server means is adapted to implement the MILENAGE algorithm.

15. A method for use of internet authentication technology to provide UMTS authentication, the method comprising:

providing Serving GPRS Support Node (SGSN) means in a UMTS network; and

providing RADIUS server means,

15 signalling between the SGSN means and the RADIUS Server means so that authentication of a User Subscriber Identity Module (USIM) is performed in the RADIUS Server means.

20 16. The method of claim 15 wherein the SGSN means is integrated with Radio Network Controller (RNC) means in Integrated Network Controller (INC) means.

17. The method of claim 15 or 16 wherein the UMTS network comprises a UMTS Terrestrial Radio Access Network (UTRAN).

18. The method of any one of claims 15-17 wherein the SGSN means sends an Access-Request RADIUS message to request a UMTS Authentication Vector from the RADIUS server means.

30

- 21 -

19. The method of any one of claims 15-18 wherein the
RADIUS Server means generate authentication and keying
material so as to authenticate a USIM within a UMTS UE,
5 according to UMTS standards.

20. The method of claim 19 wherein the RADIUS Server
means implements the MILENAGE algorithm.

10 21. The method of claim 19 or 20 wherein the RADIUS
Server means generates, using anti-replay-attack dynamic
data, a UMTS Authentication Vector and sends the it to
the SGSN means.

15 22. The method of claim 19 when dependent on claim 18
wherein the RADIUS Server means supports dynamic sequence
number (SQN).

20 23. The method of any one of claims 15-22 wherein the
RADIUS Server means generates a UMTS Authentication
Vector in a RADIUS attribute within an Access-Accept
RADIUS message and sends it to the SGSN means.

25 24. The method of any one of claims 15-23 wherein the
SGSN means receive a UMTS Authentication Vector in a
RADIUS Access-Accept message.

30 25. The method of any one of claims 15-24 wherein the
SGSN means sends information to re-synchronise anti-
replay-attack information within the USIM with the RADIUS
Server means.

- 22 -

26. The method of claim 25 when dependent on claim 18 wherein the SGSN means sends a UMTS-Resynchronisation-Token attribute in the Access-Request RADIUS message.

5

27. The method of claim 26 wherein the RADIUS Server means resets anti-replay-attack dynamic data in-line with the USIM in response to the data received in the UMTS-Resynchronisation-Token.

10

28. The method of claim 27 wherein the RADIUS Server means implement the MILENAGE algorithm.

29. A RADIUS Server adapted to perform the method of any
15 one of claims 15-28.

30. A SGSN adapted to perform the method of any one of claims 15-28.

20 31. A computer program element comprising computer program means for performing the method of any one of claims 15-28.